Remarks and Arguments

Claims 1-30 were presented for examination. Claim 21 has been amended.

Claims 21-30 have been rejected under 35 U.S.C. §101 for being directed to non-statutory subject matter. In response, claim 21 has been amended to recite, in lines 3-4, "… the computer program product comprising a computer usable storage medium …" making it clear that the recited program code is stored in a memory device. Consequently, amended claim 21 is believed to recite statutory subject matter. Claims 22-30 were presumably rejected for their dependency on a rejected claim. As claim 21 is now believed to be statutory, the rejection of claims 22-30 is hereby respectfully traversed.

Claims 1, 3-7, 10, 11, 13-17, 20, 21, 23-27 and 30 have been rejected under 35 U.S.C. 102(e) as anticipated by U.S. Patent No. 6,449,721 (Pensak.) The examiner comments that the Pensak reference discloses all of the claimed limitations.

The present invention relates to delivery of content to an unsecure site. Rather than downloading each content document on demand from the publisher location to the site, at the publisher location, each content document is encrypted and a document identifier is computed for that document. The document identifier is computed so that it identifies the encrypted file using the encrypted data, but cannot be derived from the encrypted data in the file alone. The document identifier is associated with the decryption key for that document. Then multiple encrypted documents with their decryption keys are assembled into a distribution archive that is also encrypted. The distribution archive is then downloaded to a local content server at the unsecure site. When the content server receives the distribution archive, it decrypts the archive file and unpacks the encrypted documents, but does not decrypt each document. Instead, the encrypted documents are stored in encrypted form in a local content server.

A user can then log on to the local content server with a document viewer and request a selected document by referring to the document name or URL. The server retrieves the encrypted document from the local document database and forwards it to the viewer in encrypted form. The viewer then computes a document identifier from the encrypted document content and uses the identifier to request a key from the server in order to decrypt the document. .

9

The key is then forwarded from the server to the viewer, which then decrypts the document and displays it in the viewer. Since the document is processed by the viewer and displayed only in a window associated with the viewer, when the viewer runs in a conventional browser, none of the browser functions has to be disabled. Further, since the document is downloaded in encrypted form, it cannot be stored or forwarded using the conventional browser.

The Pensak reference discloses a digital rights management system in which an authoring tool used by a document author divides a document into segments and generates a segment ID unique to each segment. The segment IDs are then sent to a remote server where an encryption key and a corresponding decryption key are generated for each segment ID. The encryption keys are sent back to the author and the decryption keys are stored in the remote server along with a set of access rights that govern who may view that segment. The author then uses the encryption keys to encrypt the corresponding segment. When done, the author generates a hash of the entire encrypted document and sends the hash to the remote server as a document identifier.

A viewing user then makes a request to the remote server to view a document. Pensak does not describe how this request is made other than to state that the viewing tool asks for the decryption key for first document segment. The content server uses the segment ID of that document segment to determine whether the viewing user has access rights. If the viewing user does have access rights, the segment ID is used to retrieve the decryption key which is then sent to the viewing tool. The viewing tool decrypts the encrypted segment. It is also not clear how the viewing user obtains the encrypted document segment.

Thus, the operation and construction of the Pensak system differs from the present invention. These differences are recited in the claims. Claim 1 is illustrative. It recites, in lines 6-8, "… computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document …" The examiner cites Pensak column 2, lines 18-65; column 3, lines 19-30 and column 7, line 6 to column 8, line 67 as disclosing this step. This section of Pensak refers to the aforementioned document

10

segment IDs. However, it is clear from the <u>Pensak</u> disclosure that the document segment IDs in <u>Pensak</u> are not calculated from the encrypted document content, as recited, since they are sent from the authoring tool to the remote server before the encryption process takes place in order to obtain the encryption and decryption keys. Instead, "unique" segment IDs are assigned to each document segment by the authoring tool before encryption takes place. Although the <u>Pensak</u> authoring tool does compute a document ID from the encrypted document contents, this document ID is a simple hash of the encrypted contents. This document ID is computed from the encrypted document content, but, contrary to the recitation of claim 1, it can be derived solely from the encrypted version of the requested document. Thus, claim 1 patentably distinguishes over the cited reference.

Claims 3-7 and 10 are dependent, either directly or indirectly on claim 1 and incorporate the limitations thereof. Therefore, they distinguish over the cited reference in the same manner as claim 1. In addition, these claims recite additional limitations not disclosed in the cited reference. For example, claim 3 recites that the document identifier is computed from the encrypted document content and a text string at the publisher site. The examiner cited <u>Pensak</u> column 3, lines 19-30. However, this section of <u>Pensak</u> refers to the document segment IDs which, as discussed above, are not calculated from the encrypted document content. Therefore, claim 3 distinguishes over the <u>Pensak</u> reference for this reason also.

Claims 11 and 21 recite limitations that parallel those in claim 1 and distinguish over the cited reference in the same manner as claim 1. Claims 13-17, 20 and 23-27, 30 are dependent, either directly or indirectly on claims 11 and 21, respectively, and incorporate the limitations thereof. Therefore, they distinguish over the cited reference in the same manner as claims 11 and 21. In addition, claims 13 and 23 recite limitations that parallel those in claim 3, discussed above. Therefore, they also distinguish over the cited reference in the same manner as claim 3.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, he is invited to call applicants' attorney at the number listed below. The examiner is hereby authorized to

11

charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to Deposit Account number 50-3969.

Respectfully submitted

_____/paul e. kudirka/_____Date:___2007-04-11_____
Paul E. Kudirka, Esq. Reg. No. 26,931
LAW OFFICES OF PAUL E. KUDIRKA
Customer Number 64967
Tel: (617) 357-0010 Fax: (617) 357-0035